SYSTEM AND METHOD FOR SECURE MESSAGE REPLY

FIELD OF THE INVENTION

The present invention relates to a system and method for securely providing a reply via the Internet in response to an online submission made by an unregistered user. More particularly, but not by way of limitation, the present invention is a system and method for securely providing a reply containing private information to a prospect who has submitted an online submission and/or inquiry via a website without having the prospect first pre-register or establish an account.

BACKGROUND OF THE INVENTION

There is a need by organizations, such as businesses, to provide secure responses not only to an established customer, but also to an unregistered user or prospect. The prospect includes, for example, a unauthenticated visitor at a website who does not have an account with the organization associated with the website. The term "account" is not intended to be limiting and can apply to any type of record or documentation on the user, including, for example, in the context of a banking website, a credit card account, checking account, etc.

Although the capability to securely accept communications via the Internet may exist, there is not an effective and efficient way to reply to an unregistered prospect via the Internet in a secure form so that the prospect may remain anonymous. Therefore, private and/or confidential information is not included in replies to

unregistered prospects via the Internet. Secure replies are limited to those registered users who have been authenticated and have an established account. Further, there is not an efficient and cost-effective way to incorporate existing infrastructure to provide the secure replies to the unregistered users.

Accordingly, there is a need for a system and method for securely providing a reply via the Internet in response to an online submission made by an unregistered user or prospect.

SUMMARY OF THE INVENTION

An embodiment of the present invention is a system and method whereby an unregistered user or prospect may go to an organization's website with a submission or inquiry, and receive a secure response from the organization without establishing an account with the organization. There is no requirement for the prospect to "log on." The submission may be, for example, a loan application made to a financial services institution. The loan application by the unregistered prospect may contain private information about the prospect which he/she sends via a secure website. The response from a customer service representative at the financial services institution is also provided in a secure manner via the Internet, although the prospect did not pre-register and remains anonymous. The response may include the prospect's private information that was in the original submission, such as, an account number, a balance, or other additional private information. Although reference is made to the

Internet, other communication systems are also within the scope of the invention.

An embodiment of the present invention provides that the prospect enter a prospect-created password as part of the original submission. In a further embodiment, the password is required to satisfy certain security requirements in terms of length and character combinations so that it cannot be easily guessed by another person. A secure relationship is created on a per-submission basis. For each submission he/she sends via the website, the prospect can use a different password (a different identification). The prospect is able to retrieve a return message in a secure manner because he/she is the only one who knows what was entered as the password. The prospect remains anonymous in the transaction to protect his/her privacy. Other embodiments include providing a user name along with a password, wherein the user name is the email address of the prospect. A different email address may also be provided by the prospect as the user name. Other embodiments involve passwords and/or other types of identifiers that have been provided to the prospect.

An embodiment of the present invention comprises the following steps: A user at a personal computer, kiosk, etc. enters a website, for example a website of a mortgage lender, and completes a "contact us" form wherein the user identifies himself/herself and provides specific information. The user provides a shared password for that particular communication. In this embodiment, the information is sent to an Internet Email Workflow Application (IEWA). A customer service representative, after verifying the user and the required data, prepares a reply to the

user. A copy of the reply is placed in the web server. The reply may be made available for only a specified period of time, for example, 30 days. A notification email is sent (e.g., Simple Mail Transfer Protocol) to the user to securely retrieve the reply without any additional information. The notification, for example, takes the form of providing the user with a hyperlink of a Uniform Resource Locator in the notification email and an authentication screen is displayed whereby the user is asked for his/her identification and a password. Once authenticated, the secure reply is presented to the user.

Although examples of certain types of online forms have been identified, these examples are not meant to be limiting. There are countless varieties of online forms that may be used, such as, online forms pertaining to credit cards, loans, change of addresses, registration, identification, resumes, surveys, technical problems, etc.

As discussed, an embodiment of the present invention provides for a secure dialogue on a per submission/inquiry basis. The same prospect may complete a second online form and provide a different email address as an identifier and a different password. There is no need for the prospect to register or establish a universal account. A level of anonymity is therefore maintained and privacy is enhanced. Further, the person accessing the website need not be a first-time prospect but may be an existing customer, and the submission need not be an online form but can be any type of submission pertaining to a variety of matters.

A further embodiment of the invention is a method for providing a secure response to a first party, comprising the steps of: receiving a submission from the first party over a communications network, wherein the submission is directed to a second party and includes an identifier associated with the submission, and wherein the first party has not established a relationship with the second party. The steps further include receiving a response to the submission from the second party, storing the response for later retrieval by the first party or the second party, and sending a notification to the first party wherein the notification provides information for securely accessing the response. The steps also include receiving a second submission from the first party wherein the second submission comprises information for correlation to the identifier provided in the first submission, authenticating the first party, and permitting the first party to securely access the response from the second party.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:

FIG. 1 is a system architecture diagram of an embodiment of the invention; and

FIG. 2 is a system architecture diagram of an alternative embodiment of the invention.

DETAILED DESCRIPTION

Reference will now be made in detail to embodiments of the invention, one or more examples of which are illustrated in the accompanying drawing. Each example is provided by way of explanation of the invention, not as a limitation of the invention. It will be apparent to those skilled in the art that various modifications and variations can be made in the present invention without departing from the scope or spirit of the invention. For instance, features illustrated or described as part of one embodiment can be used on another embodiment to yield a still further embodiment. Thus, it is intended that the present invention cover such modifications and variations that come within the scope of the invention.

In an embodiment of the present invention, communication is submitted by a user visiting a web site. The communication may be, for example, forms-based, meaning a form with a preset design, such as an online application form or customer service communication form. The embodiment further comprises a secure e-mail messaging system, such as, an Internet Email Workflow Application (IEWA) that supports two way messaging and allows a business to receive and process customer communications sent via the web site. Communication from the Internet user is secured using, for example, SSL with 128-bit encryption.

Once a response has been prepared to the user's submission, communication to the user is made via an unsecured e-mail notification that provides the user with an

HTTPS link to an authentication page. The user then enters his/her user identification, for example, the user's email address and password which was associated with the original submission. Once the email address and password are authenticated, the secure response message is displayed on the user's web browser in SSL.

Referring now to Fig. 1, the user (customer, prospect, etc.) through his/her web browser 1 visits a web site and provides a submission, for example, by filling in and submitting an online loan application form, using a secure connection (SSL) 2. The web server 3 hosting the web site converts the form into an email message, then encrypts the message 4, for example, using Entrust, and sends it, for example, to the IEWA Domino Server 5. If a password is included in the user's submission, and a customer service representative (CSR) 6 chooses to send a secure response 6a to the user, the following process takes place in accordance with an embodiment of the invention.

IEWA saves the secure response in the secure response database residing on the same Domino server 5 as the workflow database. Also, the secure response message is saved in the history section of the original message. A notification message 7, configurable by workflow administrators, is sent to the user's email address with instructions on how to access the secure response via a web browser in SSL connection. If the above notification message 7 is bounced, IEWA locates the original message in the workflow database and marks the message status as bounced.

When the user attempts to retrieve 8, 8a the secure response in a SSL session using the link provided in the notification message, he or she is prompted to enter the email address and password that was provided in his or her initial request message. The page will make HTTPS connections 9 to the IEWA Domino Server for the secure response content. If the email address and password combination is correct, the response message will be displayed on the user's web browser in SSL. Otherwise, the user will be asked to reenter the email address and the password. If the user fails to provide the correct combination for, for example, six consecutive times, the secure response will be disabled/locked from the secure response database. Time and status of the user's attempts to retrieve the secure response is recorded in the history section of the original message. Regardless of user success or failure to retrieve the response message, the secure response is disabled/locked in the secure response database after, for example, seven days. IEWA removes the disabled/locked secure response from the secure response database after a specified number of days.

Fig. 2 is an alternate embodiment of the invention and illustrates that the system architecture need not involve separate web servers as depicted by the embodiment in Fig. 1.

Embodiments of the present invention have now been described in fulfillment of the above objects. It will be appreciated that these examples are merely illustrative of the invention. Many variations and modifications will be apparent to those skilled in the art. Although examples have been provided in the context of private

information related to financial matters, the invention is not limited as such and is also applicable to private information related to, for example, health and other personal matters.